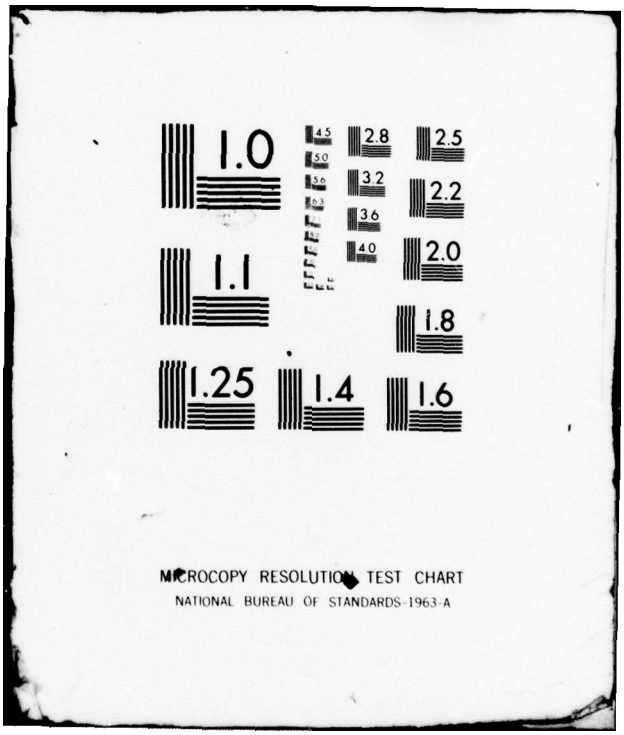
AD-A071 729 HAWAII UNIV HONOLULU DEPT OF ELECTRICAL ENGINEERING F/G 17/2
DEFENSE PACKET SWITCHING NETWORKS IN THE UNITED STATES,(U)
1979 F F KUO N00014-78-C-0498

UNCLASSIFIED NL

| OF |
AD
A071729

END
DATE FILMED
8-80
DTIC


1.0
1.1
1.25
1.4
1.6
2.8
2.5
3.2
2.2
3.6
2.0
4.0
1.8
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

DEFENSE PACKET SWITCHING NETWORKS IN THE UNITED STATES*

Franklin F. Kuo

Dept. of Electrical Engineering
University of Hawaii
Honolulu, HI 96822 USA
formerly of the Office of the Secretary of Defense
Washington, D.C.

ABSTRACT

In this paper we review the primary characteristics of the U.S. Department of Defense packet switching networks -- ARPANET, AUTODIN II, and WIN. Special requirements for dedicated defense networks are examined. These include privacy and security, precedence, survivability, availability, and interoperability with other networks. Finally, we discuss some architectural concepts for an all digital integrated voice/data network for defense applications in the 1990's.

1. INTRODUCTION

Department of Defense data communications systems have special performance requirements which are perhaps more stringent than commercially available systems. These requirements concern survivability, availability, security, precedence, and interoperability with other Defense networks of the US and NATO Allies. Because of these special requirements, the Defense Department has its own "common-user" networks--AUTOVON, a circuit-switched voice network, AUTOSEVOCOM, a secure voice network, and AUTODIN I, a store-and-forward message-switched network. In addition to these common-user networks, a number of other special purpose Defense networks exist because of special security or capacity requirements which the common-user networks are unable to meet.

*This work sponsored by the Office of Naval Research under Contract N00014-78-C-0498

D. REIDEL PUBLISHING COMPANY / DORDRECHT, HOLLAND / BOSTON, U.S.A.

With packet switching emerging as an attractive, cost effective technology for data communications, the Defense Department is presently operating or developing a number of new packet-switching networks--ARPANET, AUTODIN II and WIN. It is the purpose of this paper to discuss some of the features of these networks and examine some of the requirements that place special demands on these defense networks.

2. SPECIAL REQUIREMENTS ON DEFENSE DATA NETWORKS

Survivability

Defense data networks must be survivable in the event of nuclear attack. This places special requirements on the location of switching centers, routing of transmission links, and protection of satellite and radio links against enemy jamming. Most U.S. military switching centers, although located in guarded and secure areas, are nevertheless vulnerable to direct hits. To maintain connectivity, such techniques as poly-grid networks, diverse routing, and alternate forms of communications are used.

Privacy and Security

In US military communications the sensitivity of information is protected by a security classification system which prescribes the safeguards required. The security levels of military messages are: TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED. If a communications system is required to handle all the four categories of traffic, there are special design requirements on the switches to insure that the security safeguards are not compromised. Until a provable secure operating system can be realized to provide multi-level security, the multiplicity of security checks that must be performed in a communications processor place a severe overhead burden on processor operation. Security is a primary reason why military messages are not sent on commercial networks. Within the next ten years, end-to-end encryption systems will be perfected which use remote key distribution [1]. With the use of these systems, it will be possible to send the bulk of sensitive military traffic on commercial networks.

Availability and Precedence

Among military messages, some messages are more critical than others, and must be transmitted and received more quickly than the less critical messages. Thus in military communications, a system of *precedences* is used in which messages have a priority

in the order: FLASH OVERRIDE, FLASH, IMMEDIATE, PRIORITY, and ROUTINE. In a military packet switching network, every packet transmitted must have the precedence designation in the header field. These precedence protocols are generally absent in non-military applications.

During a state of national crisis or emergency, public telephone systems become overloaded quickly. Military communication systems must be designed with sufficient excess capacity to handle the severe load demands placed upon them during crisis situations. They must be able to operate even when major switching centers and transmission links become severed. Availability is thus a primary requirement for military communication systems and one which dictates in some instances the use of dedicated circuits, rather than common user networks. For it is easy to imagine that in a severe crisis situation even military common user networks can get flooded with high precedence traffic and thus become unavailable.

Interoperability

Up to the present, little attention has been paid to the issue of interoperability between defense data networks. Thus in most instances, dedicated networks do not interface with common-user networks. The US Department of Defense policy is to employ common-user networks whenever feasible. AUTODIN II is being developed in order to stop the proliferation of specialized data networks for specific applications such as logistics. WIN, although a dedicated network for command and control, was developed before AUTODIN II was approved, and it will be subsumed when AUTODIN II becomes fully operational. It should be mentioned here that although AUTODIN II uses an early version of the internet protocol TCP developed by Cerf and Kahn [2], AUTODIN II cannot interoperate with networks operating with the X-25 protocol [3].

Interoperability requirements become more severe in a NATO environment. The NATO Integrated Communications System does not at present interoperate with the many national defense communication systems. There are urgent requirements for interoperability among NATO nations that are not met. NATO planning for interoperability of national defense communications networks should be a task of the highest priority.

3. ARPANET, AUTODIN II AND WIN

In this section we will examine briefly the features of the DoD packet switching nets: ARPANET, AUTODIN II and WIN and then discuss certain issues associated with the networks.

D. REIDEL PUBLISHING COMPANY / DORDRECHT, HOLLAND / BOSTON, U.S.A.

1st line of text

ARPANET

In 1968 the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense began implementation of a computer-communication network which permits the interconnection of heterogeneous computers at geographically distributed centers throughout the United States. This network has come to be known as the ARPANET [4], and has grown from the initial four node configuration in 1969 to over forty nodes (including satellite nodes in Hawaii, Norway, and London) at present. The major goal of ARPANET is to achieve resource sharing among the network users. The resources to be shared include not only programs, but also unique facilities such as the powerful ILLIAC IV computer and large global weather data bases that are economically feasible when widely shared. Today the ARPANET provides support for a large number of DoD and other government projects with an operational network of many nodes and host computers. Responsibility for the operation of the ARPANET was transferred from ARPA to the Defense Communications Agency (DCA) on July 1, 1975.

AUTODIN II

AUTODIN (Automatic Digital Network) II is a new DoD common-user packet switching network which will provide the capability of transferring information between DoD data processing centers and remote user terminals. Initially AUTODIN II will consist of eight switching centers located in the continental US which are connected by 56 KB links. Access to these nodes can be direct or via lower speed lines connected to concentrators and multiplexors. It must be emphasized that the AUTODIN communications processors are high speed, high capacity devices which can connect to many host computers rather than the four that the ARPANET IMPs permit. A 1976 estimate of the potential users of AUTODIN II indicate that there will be over 160 host computers and over 1300 terminals connected to AUTODIN II, thus, illustrating the point that there will be a far greater density of users/node in AUTODIN II than ARPANET. Users of AUTODIN II will include members of the DoD command and control, intelligence, and logistics communities as well as environmental services and Army, Navy, Air Force management information systems. AUTODIN II will be designed with provisions for security, priority control, and establishment of close communities of interest. To summarize, AUTODIN II is a leased, industrially funded packet switching common-user network that is designed to a higher level of reliability, survivability and throughput than ARPANET.

A contract for the development and lease of AUTODIN II was awarded to a team consisting of Western Union, Computer Science Corporation and Ford Aerospace in November 1976. The system is

24 pi

Catchline/Foot

D. REIDEL PUBLISHING COMPANY / DORDRECHT, HOLLAND / BOSTON, U.S.A.

Reduction

expected to be in an initial operational phase with four nodes by late 1979. One node per month will be added after completion of the operational testing period. The network is expected to be extended to Europe and the Pacific in the early 1980's.

WIN

WIN is an acronym for WWMCCS Intercomputer Network. WWMCCS is an acronym for World Wide Military Command and Control System, which among its many facilities, includes the WWMCCS ADP (Automatic Data Processing) System. [5] The WWMCCS ADP system includes 35 medium and large scale computer systems and remote terminals at 26 locations around the world. The 35 systems are intended to function as an integrated worldwide system with common hardware: (Honeywell 6000 miniframes, DATANET 355 front ends, 716 remote minis, VIP 7700 terminals, etc); common system (GCOS III) and applications software, data bases, and centralized management, support and planning.

Up to 1975, these WWMCCS computers were not connected by a computer network. In 1974-76 an earlier version of WIN called PWIN was developed as a secure, mini-version of ARPANET which connects six WWMCCS ADP sites together for command and control applications. WIN uses modified ARPANET IMPs as its communications subnet computer. These IMPs are interfaced to the Honeywell 6000 host computers using Honeywell DATA-NET 355 front end processors. Remote terminal access to WIN is also possible through the 355's. Since WIN is restricted to classified command and control applications, communications security is provided by KG-34 cryptographic devices. These devices encrypt and decrypt all information sent between network links to prevent unauthorized access to the classified military information being transmitted by WIN users, all of whom possess top-secret clearances. Thus WIN can be regarded as a secure version of ARPANET.

The following capabilities of WIN are key:

- TELNET - enables the user to access PWIN computers which are geographically remote
- TELECONFERENCE - enables a teletype conference to be conducted among users at different WIN sites
- SENDFILE - enables data files to be moved between computers at various WIN sites

WIN presently utilizes dedicated 50 KB lines. It is anticipated that it will utilize the new DoD packet switching network, AUTODIN

D. REIDEL PUBLISHING COMPANY / DORDRECHT, HOLLAND / BOSTON, U.S.A.

II, as a backbone network when AUTODIN II becomes operational in late 1979.

The Future of these Networks

It is difficult to predict when AUTODIN II will become fully operational. When it does achieve operational status, however, military users of ARPANET can switch over to AUTODIN II, where they can operate in a secure mode. (Selected ARPANET traffic can be secured but at considerable expense). WIN will be subsumed by AUTODIN II. Only the highest level WIN protocols will remain since WIN users will represent a close community of users within AUTODIN II. The communications functions of WIN will be completely taken over by AUTODIN II.

The future of ARPANET is considerably more uncertain than that of WIN. ARPANET is still considered an experimental network that both the research community and the military users share. If the military users are all rehomed on to AUTODIN II, many of the research users can go onto a commercial packet switching network such as TELENET [6]. However networks such as TELENET are operational and not experimental nets and it is as difficult to change the transmission protocols on these networks as for operational military networks such as AUTODIN. Thus a special subset of ARPANET users will require the continued existence of ARPANET in order to carry out their research in such areas as internetting, packet satellite and packet speech protocols. Because of the diverse community it serves, it is difficult to imagine that ARPANET could be readily subsumed by AUTODIN II. Some alternatives that are presently being explored are:

1. Leave ARPANET as presently constituted and gateway it to AUTODIN II.

2. Arrange for gateway connections between ARPANET and a public packet switching net.

Much research needs to be carried out on access control and network security before a public packet switching network and AUTODIN II can be connected via a gateway.

With such issues presently under discussion, the future of ARPANET is unclear.

4. THE INTEGRATED AUTODIN SYSTEM

The Integrated AUTODIN System (IAS) is the future all-digital, wideband, US defense communications system permitting global com-

D. REIDEL PUBLISHING COMPANY / DORDRECHT, HOLLAND / BOSTON, U.S.A.

munications between humans in either voice (secure or unsecure) or record, between men and computers, and between computers. The near-term architectural objectives of IAS include:

1. Functional specifications for a common family of AUTODIN terminals

2. ARPANET Transition

3. Integration of AUTODIN I into AUTODIN II

4. Extension of AUTODIN II overseas

The far-term architectural objectives of IAS include a number of research and development tasks such as:

1. Development of packet broadcast satellite techniques [7].

2. Development of end-to-end encryption and other network security techniques.

3. Development of gateway techniques.

4. Development of local and regional access nodes.

Most of the R & D tasks are expected to be completed by 1990, when a candidate architecture for the future IAS will be considered. It is expected that the IAS will be heavily dependent upon packet switching techniques and that AUTODIN II will be a major component of the IAS.

5. REFERENCES

[1]. S.T. Kent "Security in Computer Networks" in Protocols and Techniques for Data Communication Networks, F.F. Kuo ed., to be published by Prentice-Hall, 1979.

[2]. V.G. Cerf and R.E. Kahn "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, COM-22, May 1974, pp. 637-648.

[3]. A. Rybcznshi, B. Wessler, R. Despres and J. Wedlake, "A New Communication Protocol for Accessing Data Networks - The International Packet-Mode Interface" Proceedings of the National Computer Conference, AFIPS Conference Proceedings Vol. 45, June 1976, pp. 477-482.

[4]. L.G. Roberts and B.D. Wessler, "Computer Network Development to Achieve Resource Sharing" Proceedings 1970 SJCC, Montvale, NJ: AFIPS Press, pp. 543-599.

[5]. H.B. Goertzel and J.R. Miller "WWMCCS ADP: A Promise Fulfilled", Signal, Vol. 30, No. 8, May 1976, pp. 57-63.

[6]. B.D. Wessler and R.B. Hovey, "Public Packet-Switched Networks", Datamation, July 1974, pp. 85-87.

[7]. I.M. Jacobs, R. Binder, E. Hoversten "General Purpose Packet Satellite Networks", Proceedings IEEE, November 1978.